REMARKS

Claims 14-28 and 37-44 are pending in this application, all of which stand rejected as a result of the February 27, 2006 Office Action. Claims 14-19, 21-28, and 37-44 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,718,361 (Basani) in view of U.S. Patent Application No. 2002/00022611 (Vange), and in further view of U.S. Patent No. 6,892,306 (En-Seung). Claim 20 has been rejected under section 103(a) as being unpatentable over Basani as modified by Vange and En-Seung in further view of U.S. Patent No. 6,425,017 (Dievendorff). Applicants respectfully disagree with the grounds for rejection and traverse.

Independent Claim 14

Claim 14 recites various features concerning the use of three cryptographic keys (a "public key," a "first key," and "second key"). In particular:

- A "first server" generates a request that (1) represents the public key, and (2) is encrypted with the first key
- The first key is known to the first server and to a plurality of download servers, but is not known to a user
- A content item has (1) content encrypted with a second key, and (2) the second key encrypted by the public key.

The Examiner has read these features onto En-Seung. It should be noted that, while claim 14 is rejected under section 103, the Examiner has not asserted that En-Seung (or any of the other references used in the rejection of claim 14) motivates a modification that would yield the above-mentioned features. Rather, the Examiner relies solely on the argument that En-Seung teaches the above-mentioned features, and that En-Seung's teachings should be combined with Basani and Vange.

In essence, the features summarized in the bullet points above define a specific relationship between the public key, first key, second key, first server, plurality of download servers, and the user. En-Seung does not teach these features, or the claimed relationship between them. In particular, the Examiner finds that En-Sung's receipt of "key information" corresponds to the "request" of claim 14, and that the "key information" corresponds to the

"public key" represented in the request. The Examiner is not entirely clear as to what component of En-Sung constitutes the "first key" that is used to encrypt the request, although it appears that the Examiner's position is that, when En-Seung's "key information" is generated "in dependence upon the user's identity characters," the key information has been somehow encrypted by the identity characters. There is actually no suggestion in the applied portion of En-Sung that the identity characters are used to encrypt the "key information." Nor does such a suggestion appear in any other portion of En-Seung that applicants have been able to identify. However, for only the purpose of discussing the Examiner's reasoning, applicants will assume that that "key information" is claim 14's "public key", and that the "identity characters" are claim 14's "first key."

It is at this point that the Examiner's logic fails. Under the above correspondence, the Examiner would have to demonstrate (based on the claim features shown in the second bullet point above) that the "identity characters" are known to a first server and to a plurality of download servers, but not to the user. As to this feature, the Examiner cites col. 8, lines 15-30 of En-Seung – in particular, the portion that states that the user authorization identifier 202 "obtains the user's key after reading the header of the copyright protection protocol received from service server 210." It should be noted that the Examiner has switched which component of En-Seung corresponds to the claimed "first key." Initially – as described above in the preceding paragraph – the claimed "first key" is the "identity characters." Later, it appears that the claimed "first key" is the "user's key." However, it makes no difference which position the Examiner is taking, since there is no suggestion that either the "identity characters" or the "user's key" in En-Seung are "known to said first server and to said plurality of download servers but not to said user." It would be essentially impossible for the "identity characters" to be unknown to the user, since, in En-Seung, these identity characters preferably constitute either the user's social security number, or driver's license number, or resident registration number. (Col. 7, ll. 28-32.) Second, as to the "user's key," there is simply no indication of who that key is known to – much less that it is specifically known to a first server and a plurality of download servers, but not to the user himself. Thus, the Examiner has not demonstrated that En-Seung teaches the features mentioned in the second bullet point above.

Additionally, in order to read claim 14 onto En-Seung, the Examiner would have to show that En-Seung teaches content encrypted with a second key, where the second key is encrypted with the public key (which, in the Examiner's reasoning, is En-Seung's the "key information".) The applied portion of En-Seung does mention that content can be decrypted using a temporary validation key, and the Examiner does appear to state that En-Seung's temporary validation key corresponds to the claimed "second key." However, the temporary validation key is not encrypted by the "key information." Thus, the relationship between the temporary validation key and the key information is not the same as the relationship between the public key and first key in claim 14.

Applicants note that the Examiner has not attempted, in the present office action, to read the features summarized in the above bullet points onto any reference other than En-Seung. However, applicants note that none of the other applied references teach or suggest these features.

Accordingly, applicants submit that claim 14 is patentable over the applied references, and applicants request that the Examiner reconsider and withdraw the rejection.

Independent Claim 21

Independent claim 21 recites that there are a plurality of servers that share knowledge of a first key with a "first server" at which a request is generated. The request generated at the first server comprises a public key in a form encrypted by a first key. The public key is installed on a plurality of machines associated with a particular user. While claim 21 is not identical in scope or language to claim 14, it shares with claim 14 the common feature that there is a "first key" known to various servers but not to a user, and that the first key is used to encrypt a public key. As to these features relating to the use of cryptographic keys, the Examiner has applied the En-Seung reference. As discussed above in connection with claim 14, En-Seung does not teach or suggest that a public key is encrypted with a first key that is shared between specific servers but that is not shared with a user. Moreover, the Examiner has cited En-Seung (at col. 5, ll. 5-20) as teaching the claim feature that the public key is installed by an activation server on a plurality of machines associated with the user. There is no suggestion in the applied passage that the public key is installed on any particular number

of machines – much less a plurality, and much less that these machines are all associated with a particular user.

It should be noted that the Examiner has not applied the features discussed above onto any reference other than En-Seung. Nor does the Examiner suggest that any of the reference motivates a modification that yields the above-described features outside of that reference's explicit or inherent teachings. However, applicants note that none of the references applied by the Examiner teaches or suggests the above-described features of claim 21; nor does any of those references motivate any modification to the references that would yield the above-referenced features.

Accordingly, applicants submit that claim 21 is patentable over the applied references, and request that the rejection of claim 21 be reconsidered and withdrawn.

Independent Claim 37

Independent claim 37 recites that a request is received at one of a plurality of servers from a "remote" server; that the request comprises a public key associated with a user; that the request is encrypted with a first key; that the first key is known to the remote server and the plurality of servers, but not to the user; that a content item identified in the request is encrypted so as to be decryptable by with the first key; and that the first key is contained in the content item in a form decryptable with the public key.

While claim 37 is not identical to claims 14, and 21 in either language or scope, claim 37 recites features that are similar to some of the features relating to the use of keys discussed above in connection with claim 14. The Examiner has, again, relied on En-Seung for its alleged teachings of these features. For essentially the reasons discussed above in connection with claims 14 and 21, En-Seung does not teach the particular use of keys recited in claim 37, and neither do any of the other applied references.

For the foregoing reasons, applicants request that the rejection of claim 37 be reconsidered and withdrawn.

Claim 16

Claim 16 is dependent on claim 14, and further recites that the user has engaged in a purchase transaction with a first server, where the first server includes functionality to

determine whether to generate a request (or not to generate the request) depending on whether the user has completed said purchase transaction. In prior Office Actions, the Examiner had relied on Vange, then Tarpenning (U.S. Patent No. 6,513,117), and now relies on En-Seung (specifically, at col. 7, ll. 22-60). However, the applied portion of En-Seung merely mentions that the user has obtained content and that fees have been collected. There is no suggestion that a server determines whether to generate, or not generate, a request depending on whether the user has completed a purchase transaction. Rather, it is assumed in the applied portion of En-Seung that the user has completed the transaction since the user is being charged fees. Moreover, there is no reason why En-Seung would determine whether a purchase transaction has been completed prior to generating a request for content, since En-Seung does not control access to content by determining whether to generate an encrypted request for that content. In the present application, one of the ways that the user's right to obtain the content is established by the user's being in possession of an encrypted, authenticatable request for the content, and En-Seung simply does not work in this manner.

Accordingly, the newly-cited En-Seung reference fails to teach the features of claim 16, and does not address the deficiency in the prior Office Actions' various reliance on Vange and Tarpenning. Accordingly, applicants requests that the rejection of claim 16 be reconsidered and withdrawn.

Claims 19 and 24

While claims 19 and 24 are not identical in either language or scope, both of these claims recite limits as to the number of machines on which a public key associated with a user can be installed.

As to these features, the Examiner has relied on En-Seung, – in particular, col. 6, ll. 54-67. This passage generally described the storage and use of key information on a computer. There is simply no teaching or suggestion in this passage as to a limit on the number of machines on which a public key can be installed. To the extent that the Examiner has read the claimed "public key" onto En-Seung's "key information," applicants note that there does not appear to be any suggestion in the En-Seung reference as to a limit on the number of machines on which the key information can be installed.

Thus, En-Seung does not teach or suggest the features of claims 19 and 24 for which it is cited. Applicants thus request that the rejection of claims 19 and 24 be reconsidered and withdrawn.

Conclusion

Claims 14, 16, 19, 21, 24, and 37 have been shown to be patentable over the applied prior art, and claims 15, 17, 18, 20, 22, 23, 25-28, and 38-44 are patentable at least by reason of their dependency. All issues having been addressed, applicants respectfully submit that this case is now in condition for allowance.

Date: May 25, 2006

Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439